

L Number	Hits	Search Text	DB	Time stamp
1	0	corresponding near5 file adj type with virus adj signatures	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/06/24 17:04
2	0	correspond\$6 near5 (file adj type) with (virus\$2 adj signatur\$4)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/06/24 17:05
3	0	(correspond\$6 near5 (file adj type)) with (virus\$2 adj signatur\$4)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/06/24 17:06
4	1	(correspond\$6 same (file adj type)) same (virus\$2 adj signatur\$4)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/06/24 17:10
5	0	"09581583"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/06/24 17:10
6	0	"09659864"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/06/24 17:10
7	0	"09660370"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/06/24 17:15
8	1	virus\$5 with file\$5 with type\$2 with (associat\$5 or correspond\$6) with risk	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/06/24 17:37
9	2	virus\$5 with (file\$5 or application) with type\$2 with (associat\$5 or correspond\$6) with risk	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/06/24 17:38
10	51	virus\$5 with type\$5 with categor\$5	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/06/24 17:39
-	0	NAI1P004/00.006.01	USPAT	2004/06/24 09:34
-	2	edwards.ti.	USPAT	2004/06/24 09:34
-	0	process\$1based adj selection near5 virus near5 detection	USPAT	2004/06/24 09:35
-	0	process\$1based adj selection near5 virus near5 detection	USPAT; US-PGPUB	2004/06/24 09:35
-	0	process\$1based adj selection	USPAT; US-PGPUB	2004/06/24 09:36
-	1	6393568.pn.	USPAT; US-PGPUB	2004/06/24 10:43
-	1	6393568.pn.	USPAT; US-PGPUB	2004/06/24 17:01

File 347:JAPIO Nov 1976 2003/Dec(Updated 040402)

(c) 2004 JPO & JAPIO

File 350:Derwent WPIX 1963-2004/UD,UM &UP=200430

(c) 2004 Thomson Derwent

	Items	Description
	84990	VIRUS?? OR VIRII OR VIRAL OR MACROVIRUS?? OR TROJAN()HORSE- ?? OR WORM?? OR (MALICIOUS OR HOSTILE OR SUSPECT)() (LOGIC OR - CODE OR SOFTWARE OR PROGRAM?? OR ALGORITHM? ? OR COMMAND? ? OR SIGNAL? ? OR INSTRUCTION? ?)
S2	5414	S1(5N) (SCAN???? OR DETECT? OR FIND??? OR SENS? OR IDENTIF? OR DISCOVER? OR RECOGNI????? OR DETERMIN?)
S3	3701	S1(5N) (DELET? OR ERAS??? OR EXTERMINAT? OR REMOV? OR DESTR- OY? OR KILL? OR PURG? OR ERADICAT? OR DISINFECT? OR ELIMINAT? OR CLEAR??? OR CLEAN??? OR FLUSH?)
S4	2020	(TAILOR? OR CUSTOMIZ? OR CUSTOMIS? OR INDIVIDUALIZ? OR IND- IVIDUALIS? OR PERSONALIZ? OR PERSONALIS?) (5N) (PROCESS OR PROC- ESSES OR THREAD? ? OR PROGRAM? ? OR APPLICATION? ? OR FILE? ? OR FILETYPE? ?)
S5	79655	(SPECIFIC OR CORRESPOND? OR CORRELAT? OR ASSOCIAT? OR REFE- R??? OR RELATE? ? OR RELATING) (5N) (PROCESS OR PROCESSES OR TH- READ? ? OR PROGRAM? ? OR APPLICATION? ? OR FILE? ? OR FILETYP- E? ?)
S6	3	S2:S3 AND S4
S7	117	S2:S3 AND S5
S8	41	S7 AND IC=G06F
S9	43	S6 OR S8
S10	4	S1 AND S4 AND IC=G06F
S11	2	S10 NOT S9
S12	7341	PARTICULAR(5N) (PROCESS OR PROCESSES OR THREAD? ? OR PROGRA- M? ? OR APPLICATION? ? OR FILE? ? OR FILETYPE? ?)
S13	25	S2:S3 AND S12
S14	24	S13 NOT (S9 OR S11)
S15	2344	ANTIVIRUS OR ANTI() (VIRUS OR VIRAL)
S16	21	(S4:S5 OR S12) AND S15
S17	12	S16 NOT (S9 OR S11 OR S14)

9/5/35 (Item 32 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

012907859 **Image available**
WPI Acc No: 2000-079695/200007
XRPX Acc No: N00-062960

Process execution control module of file forwarding system of distributed information processing system - initiates process controller of reception side file forwarding apparatus, to make process execution unit to execute processes according to acquired information, when file is received from transmission side system

Patent Assignee: NEC CORP (NIDE)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 11328052	A	19991130	JP 98152229	A	19980514	200007 B

Priority Applications (No Type Date): JP 98152229 A 19980514

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 11328052	A		9	G06F-013/00	

Abstract (Basic): JP 11328052 A

NOVELTY - The information about the processes to be performed are stored in memory (28) of the reception side file forwarding apparatus. When the file is received from transmission side system, a process controller (32) is initiated, for making process execution unit (30) to execute the processes according to the information acquired from the memory. DETAILED DESCRIPTION - A memory (20) of transmission side file forwarding apparatus, stores the information relevant to the processes to be performed. A process controller (24) is initiated to make the process execution unit (22) to execute the processes according to the information acquired from the memory (20). A transmitter (26) is provided for forwarding the file to the reception side system.

USE - For controlling process execution in file forwarding system of distributed information processing system.

ADVANTAGE - The file encryption, compression of file or detection of computer virus can be performed automatically during file transmission and reception, as the corresponding protocol process control information are stored beforehand in the memory of respective side file forwarding apparatus. Thus transmission of information is enabled flexibly and efficiently. DESCRIPTION OF DRAWING(S) - The figure shows block diagram of distributed information processing system having file forwarding apparatus. (20,28) Memories; (22,30) Process execution units; (24,32) Process controllers; (26) Transmitter.

Dwg.1/4

Title Terms: PROCESS; EXECUTE; CONTROL; MODULE; FILE; FORWARDING; SYSTEM; DISTRIBUTE; INFORMATION; PROCESS; SYSTEM; INITIATE; PROCESS; CONTROL; RECEPTION; SIDE; FILE; FORWARDING; APPARATUS; PROCESS; EXECUTE; UNIT; EXECUTE; PROCESS; ACCORD; ACQUIRE; INFORMATION; FILE; RECEIVE; TRANSMISSION; SIDE; SYSTEM

Derwent Class: T01; W01

International Patent Class (Main): G06F-013/00

International Patent Class (Additional): G06F-012/00 ; H04L-029/06; H04L-029/08

File Segment: EPI

9/5/36 (Item 33 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

012608081 **Image available**
WPI Acc No: 1999-414185/199935
XRPX Acc No: N99-310278

Virus checking network for multimedia communication, Internet - detects virus affected packet based on virus pattern stored in memory and

transmits bit indicating infection of packet to client side so that
corresponding file is not executed

Patent Assignee: FUJITSU LTD (FUJITSU)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 11167487	A	19990622	JP 97331409	A	19971202	199935 B

Priority Applications (No Type Date): JP 97331409 A 19971202

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
JP 11167487	A	14	G06F-009/06	

Abstract (Basic): JP 11167487 A

NOVELTY - A virus check unit (12) checks for an infected packet (Pa) by observing header, based on virus pattern stored in memory (11) in the network side. The bit (Pb) denoting infection of packet, is then transmitted towards client terminal. DETAILED DESCRIPTION - A detector (21) in client side detects infected packets, and a file execution control unit (22) prevents execution of file corresponding to infected packet. The virus pattern information is distributed through network by pattern distributing unit (31). A virus pattern management unit (32) performs single element management of virus pattern controlled by administration bureau (30).

USE - For detecting virus in internet, multimedia.

ADVANTAGE - Since virus is detected in network side, virus infection and magnification is prevented. DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of virus check network. (11) Memory; (12) Virus check unit; (21) Detector; (22) File execution control unit; (30) Administration bureau; (31) Pattern distributing unit; (Pa) Infected packet; (Pb) Bit.

Dwg.1/20

Title Terms: VIRUS; CHECK; NETWORK; COMMUNICATE; DETECT; VIRUS; AFFECT; PACKET; BASED; VIRUS; PATTERN; STORAGE; MEMORY; TRANSMIT; BIT; INDICATE; INFECT; PACKET; CLIENT; SIDE; SO; CORRESPOND; FILE; EXECUTE

Derwent Class: T01

International Patent Class (Main): G06F-009/06

International Patent Class (Additional): G06F-013/00 ; G06F-015/00

File Segment: EPI

9/5/37 (Item 34 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

012525777 **Image available**

WPI Acc No: 1999-331883/199928

XRPX Acc No: N99-249518

Virus existence indication device for network connected computer - notifies user of existence of virus when file forwarding program detects virus in data received by substitute function from socket module

Patent Assignee: NEC CORP (NIDE)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 11119991	A	19990430	JP 97303471	A	19971017	199928 B

Priority Applications (No Type Date): JP 97303471 A 19971017

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
JP 11119991	A	4	G06F-009/06	

Abstract (Basic): JP 11119991 A

NOVELTY - A hook (4) seizes a call of a socket module (2) from an application and passes the corresponding data to a substitute function (5). When a file forwarding program (1) detects existence of virus in the received data in the substitute function, a notification

unit (10) notifies user of a virus.

USE - For use during file forwarding in network connected in computer.

ADVANTAGE - Avoids unnecessary operation by user as virus existence is notified to user automatically thus safety of computer is secured.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of a automatic virus existence indication device. (1) File forwarding program; (2) Socket module; (4) Hook; (5) Substitute function; (10) Notification unit.

Dwg.1/2

Title Terms: VIRUS; EXIST; INDICATE; DEVICE; NETWORK; CONNECT; COMPUTER;

NOTIFICATION; USER; EXIST; VIRUS; FILE; FORWARDING; PROGRAM; DETECT;

VIRUS; DATA; RECEIVE; SUBSTITUTE; FUNCTION; SOCKET; MODULE

Derwent Class: T01

International Patent Class (Main): G06F-009/06

International Patent Class (Additional): G06F-013/00

File Segment: EPI

9/5/38 (Item 35 from file: 350)

MAILING(R) File 350:Derwent WPIX

© 2004 Thomson Derwent. All rts. reserv.

011776918 **Image available**

WPI Acc No: 1998-193828/199817

XPX Acc No: N98-153352

A software program or agent used in conjunction with anti- virus software to detect and remove computer viruses that may be present in electronic mail attachments - provides an interface between the message system of a network server and an anti-virus application

Patent Assignee: CHEYENNE SOFTWARE INT SALES CORP (CHEY-N); COMPUTER ASSOC

THINK INC (COMP-N)

Inventor: CHEN C; LUO C

Number of Countries: 081 Number of Patents: 016

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9810342	A2	19980312	WO 97US15661	A	19970905	199817	B
ZA 9707970	A	19980527	ZA 977970	A	19970904	199827	
AU 9742535	A	19980326	AU 9742535	A	19970905	199832	
US 5832208	A	19981103	US 96709025	A	19960905	199851	
BR 9711990	A	19991013	BR 9711990	A	19970905	200007	
			WO 97US15661	A	19970905		
CN 1236451	A	19991124	CN 97199459	A	19970905	200014	
EP 1010059	A2	20000621	EP 97940851	A	19970905	200033	
			WO 97US15661	A	19970905		
MX 9902143	A1	19990901	MX 992143	A	19990304	200067	
JP 2001500295	W	20010109	WO 97US15661	A	19970905	200107	
			JP 98512933	A	19970905		
AU 9742536	B	20010705	AU 9742535	A	19970905	200143	
KR 2001029480	A	20010406	KR 99701876	A	19990305	200162	
EP 1237065	A2	20020904	EP 97940851	A	19970905	200266	
			EP 200277028	A	19970905		
EP 1010059	B1	20030521	EP 97940851	A	19970905	200341	
			WO 97US15661	A	19970905		
DE 69722266	E	20030626	DE 622266	A	19970905	200350	
			EP 97940851	A	19970905		
			WO 97US15661	A	19970905		
RU 2221269	C2	20040110	WO 97US15661	A	19970905	200414	
			RU 99106780	A	19970905		
ES 2199372	T3	20040216	EP 97940851	A	19970905	200416	

Priority Applications (No Type Date): US 96709025 A 19960905

Cited Patents: No-SR.Pub

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

WO 9810342 A2 E 42 G06F-000/00

Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU
CZ DE DK EE ES FI GB GE GH HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT

LU LV MD MG MK MN MW NO NZ PL PT RO RU SD SE SG SI SL TJ TM TR TT
UA UG UZ VN YU ZW

Designated States (Regional): AT BE CH DE DK EA ES FI FR GB GH GR IE IT
KE LS LU MC MW NL OA PT SD SE SZ UG ZW

ZA 9707970 A 42 G06F-000/00
AU 9742535 A G06F-011/00 Based on patent WO 9810342
US 5832208 A H04L-009/00
BR 9711990 A H04L-009/00 Based on patent WO 9810342
CN 1236451 A G06F-007/02
EP 1010059 A2 E G06F-007/02 Based on patent WO 9810342

Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE

EP 1010059 A1 G06F-000/00
EP 1010059 W 43 G06F-009/06 Based on patent WO 9810342
AU 9742535 B G06F-011/00 Previous Publ. patent AU 9742535
Based on patent WO 9810342

KR 2001029480 A G06F-007/02
EP 1237065 A2 E G06F-001/00 Div ex application EP 97940851
Div ex patent EP 1010059

Designated States (Regional): AL AT BE CH DE DK ES FI FR GB GR IE IT LI
LT LU LV MC MK NL PT RO SE SI

EP 1010059 B1 E G06F-007/02 Based on patent WO 9810342
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE

DE 69722266 E G06F-007/02 Based on patent EP 1010059
Based on patent WO 9810342
RU 2221269 C2 G06F-007/02 Based on patent WO 9810342
ES 2199372 T3 G06F-007/02 Based on patent EP 1010059

Abstract (Basic): WO 9810342 A

A database (140) is used to store all e-mail (electronic mail)
messages and their **associated file** attachments, and together with
the mail server (130) comprise a message system.

The software program or agent (110) scans the attachments to all
e-mail messages handled by the mail server. The agent detaches and
forwards any message attachments to an anti-**virus** application (120)
which scans files for **viruses** and **removes** them from an infected
file. The file is then re-attached to its message by the agent.

The agent can scan both on a real-time basis and at pre-set
intervals. All e-mail messages are scanned.

ADVANTAGE - No need to be installed at every workstation due to
centralised scanning from a server, does not cause any detriment to the
e-mail attachment, and is applicable to all types of e-mail messages
including draft/stored.

Dwg.2/3

Title Terms: SOFTWARE; PROGRAM; AGENT; CONJUNCTION; ANTI; VIRUS; SOFTWARE;
DETECT; REMOVE; COMPUTER; VIRUS; PRESENT; ELECTRONIC; MAIL; ATTACH;
INTERFACE; MESSAGE; SYSTEM; NETWORK; SERVE; ANTI; VIRUS; APPLY

Derwent Class: T01

International Patent Class (Main): G06F-000/00 ; G06F-001/00 ;
G06F-007/02 ; G06F-009/06 ; G06F-011/00 ; H04L-009/00

International Patent Class (Additional): G06F-013/00 ; G06K-000/00;
H04L-012/54; H04L-012/58

File Segment: EPI

9/5/39 (Item 36 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

011763443

WPI Acc No: 1998-180353/199817

XRPX Acc No: N98-142679

Virus checking method for computer word processing application -
deactivating execution of automatic instruction sequences associated
with opened file, and detecting and examining instruction sequences at
file operation

Patent Assignee: SIEMENS AG (SIEI)

Inventor: BENEDIKT R

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
DE 19638143	A1	19980319	DE 1038143	A	19960918	199817 B

Priority Applications (No Type Date): DE 1038143 A 19960918

Patent Details:

Patent No	Kind	Lang	Pg	Main IPC	Filing Notes
DE 19638143	A1		4	G06F-012/16	

Abstract (Basic): DE 19638143 A

The method includes the steps starting a data processing application and deactivating an execution of automatic instruction sequences which may be associated with the file. A check or a query on the existence of such associated instruction sequences is performed at a file operation.

At detecting such sequence, a message is generated, which requests the execution of an instruction for processing the detected instruction sequence. The instruction sequence is processed, and depended on the result of the processing, the sequence may be deleted or executed by removing the deactivation.

USE - Esp. for detecting macro-virus in word editor, e.g. Winword, Excel, Windows applications.

ADVANTAGE - Improves protection against viruses implemented as word-processor macros.

Dwg.0/0

Title Terms: VIRUS; CHECK; METHOD; COMPUTER; WORD; PROCESS; APPLY;

DEACTIVATE; EXECUTE; AUTOMATIC; INSTRUCTION; SEQUENCE; ASSOCIATE; OPEN;

FILE; DETECT; INSTRUCTION; SEQUENCE; FILE; OPERATE

Derwent Class: T01

International Patent Class (Main): G06F-012/16

International Patent Class (Additional): G06F-011/28 ; G06F-017/21

File Segment: EPI

9/5/40 (Item 37 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

011235222 **Image available**

WPI Acc No: 1997-213125/199719

Related WPI Acc No: 1997-434688; 1998-120970; 1998-322921; 1998-399345

XRPX Acc No: N97-175742

Polymorphic virus detection in computer file using mutation-engine specific data for known polymorphic viruses - repeatedly determining if instruction is used in virus decryption loop, tagging memory location associated with instruction and scanning tagged locations for virus signatures when emulated instruction is not used in virus decryption loop

Patent Assignee: SYMANTEC CORP (SYMA-N)

Inventor: NACHENBERG C

Number of Countries: 064 Number of Patents: 006

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 9712322	A1	19970403	WO 96US15512	A	19960927	199719 B
AU 9672477	A	19970417	AU 9672477	A	19960927	199732
US 5696822	A	19971209	US 95535340	A	19950928	199804
EP 852763	A1	19980715	EP 96933930	A	19960927	199832
			WO 96US15512	A	19960927	
EP 852763	B1	20000823	EP 96933930	A	19960927	200041
			WO 96US15512	A	19960927	
DE 69609980	E	20000928	DE 609980	A	19960927	200056
			EP 96933930	A	19960927	
			WO 96US15512	A	19960927	

Priority Applications (No Type Date): US 95535340 A 19950928

Cited Patents: 3.Jnl.Ref; EP 636977

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9712322	A1	E	26	G06F-011/00	
Designated States (National): AM AT AU BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IL JP KE KG KP KR KZ LK LR LT LU LV MD MG MN MW MX NO NZ PL PT RO RU SD SE SI SK TJ TT UA UZ VN					
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG					
AU 9672477	A			G06F-011/00	Based on patent WO 9712322
US 5696822	A		13	H04L-009/00	
EP 852763	A1	E		G06F-011/00	Based on patent WO 9712322
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
EP 852763	B1	E		G06F-011/00	Based on patent WO 9712322
Designated States (Regional): DE FR GB					
EP 852763	E			G06F-011/00	Based on patent EP 852763
Based on patent WO 9712322					

Abstract (Basic): WO 9712322 A

An instruction is fetched from a computer file. Next it is determined whether the instruction is used in decryption loops generated by known polymorphic viruses identified in a list. When the instruction is used in decryption loops generated by known polymorphic viruses, a memory location associated with the instruction is tagged and the fetching and determining steps are repeated.

The method further involves scanning the tagged locations for virus signatures when the emulated instruction is not used in decryption loops generated by known polymorphic viruses.

ADVANTAGE - Detection system can be readily expanded to cover newly discovered viruses without need for extensive regression testing and modification of heuristics of emulation control module.

Dwg.2/4

Title Terms: POLYMORPHIC; VIRUS; DETECT; COMPUTER; FILE; MUTANT; ENGINE; SPECIFIC; DATA; POLYMORPHIC; VIRUS; REPEAT; DETERMINE; INSTRUCTION; VIRUS ; DECRYPTER; LOOP; TAG; MEMORY; LOCATE; ASSOCIATE; INSTRUCTION; SCAN; TAG ; LOCATE; VIRUS; SIGNATURE; EMULATION; INSTRUCTION; VIRUS; DECRYPTER; LOOP

Derwent Class: T01

International Patent Class (Main): G06F-011/00 ; H04L-009/00

International Patent Class (Additional): G06F-003/00 ; H04K-003/00

IPC Class: EPI

9/5/41 (Item 38 from file: 350)

DIALOG(R) File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

010695861 **Image available**

WPI Acc No: 1996-192816/199620

XRPX Acc No: N96-161432

Virus cleaning system in computer network - uses central management system with collation part to check agreement between virus check program conversion results

Patent Assignee: HITACHI SOFTWARE ENG CO LTD (HISF)

Number of Countries: 001 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 8063352	A	19960308	JP 94200360	A	19940825	199620 B
JP 2989487	B2	19991213	JP 94200360	A	19940825	200004

Priority Applications (No Type Date): JP 94200360 A 19940825

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 8063352	A		9	G06F-009/06	
JP 2989487	B2		9	G06F-009/06	Previous Publ. patent JP 8063352

Abstract (Basic): JP 8063352 A

The system detects the virus program residing in a specific

file . An unidirectional relation calculation part (107) computes the relation using which the virus program counter is converted. A transfer part transfers the conversion result and a registration part stores the result.

The transfer part is an integral unit of the end system (101). A central management (105) furnished with a collation part, detects whether the transferred result and the result from the relation calculation part, agrees.

ADVANTAGE - Performs virus check efficiently. Obtains result with high reliability. Obtains virus check result, automatically.

Dwg.2/5

Title Terms: VIRUS; CLEAN; SYSTEM; COMPUTER; NETWORK; CENTRAL; MANAGEMENT; SYSTEM; COLLATE; PART; CHECK; AGREE; VIRUS; CHECK; PROGRAM; CONVERT; RESULT

Derwent Class: T01

International Patent Class (Main): G06F-009/06

File Segment: EPI

9/5/42 (Item 39 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

010161281 **Image available**

WPI Acc No: 1995-062534/199509

XRPX Acc No: N95-049798

Computer virus detection system - detects viral infection of target program by emulating execution of target program and analysing emulated execution to detect viral behaviour

Patent Assignee: CHAMBERS D A (CHAM-I)

Inventor: CHAMBERS D A

Number of Countries: 006 Number of Patents: 005

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 636977	A2	19950201	EP 94305551	A	19940727	199509 B
US 5398196	A	19950314	US 9399368	A	19930729	199516
EP 636977	A3	19970806	EP 94305551	A	19940727	199743
EP 636977	B1	20010523	EP 94305551	A	19940727	200130
DE 69427252	E	20010628	DE 627252	A	19940727	200144
			EP 94305551	A	19940727	

Priority Applications (No Type Date): US 9399368 A 19930729

Cited Patents: 2.Jnl.Ref; EP 510244

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
-----------	------	-----	----	----------	--------------

EP 636977	A2	E	22	G06F-011/00	
-----------	----	---	----	-------------	--

Designated States (Regional): BE DE FR GB IT

US 5398196	A		17	G06F-015/20	
------------	---	--	----	-------------	--

EP 636977	A3			G06F-011/00	
-----------	----	--	--	-------------	--

EP 636977	B1	E		G06F-011/00	
-----------	----	---	--	-------------	--

Designated States (Regional): BE DE FR GB IT

DE 69427252	E			G06F-011/00	Based on patent EP 636977
-------------	---	--	--	-------------	---------------------------

Abstract (Basic): EP 636977 A

The behaviour analysing anti-virus program detects viral infection of a target program by emulating the execution of the program and analysing the emulated execution. The anti-virus monitor program contains both variables corresp to the CPUs registers and emulation procedures corresp to the CPUs instructions. The target program is loaded into memory and its execution is emulated by the anti-virus monitor program.

Intelligent procedures contained within the monitor program are given control between every instruction emulated so as to detect aberrant or dangerous behaviour in the target program in which case the danger of viral presence is flagged and emulation is terminated.

USE/ADVANTAGE - Emulating execution of program on computer system to detect harmful or dangerous behaviour in program e.g computer viruses.

Dwg.1b/10

File Terms: COMPUTER; VIRUS; DETECT; SYSTEM; DETECT; VIRUS; INFECT; TARGET
; PROGRAM; EMULATION; EXECUTE; TARGET; PROGRAM; ANALYSE; EMULATION;
EXECUTE; DETECT; VIRUS; BEHAVE
Derwent Class: T01
International Patent Class (Main): G06F-011/00 ; G06F-015/20
File Segment: EPI

9/5/43 (Item 40 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

009264020 **Image available**

WPI Acc No: 1992-391431/199248

Related WPI Acc No: 1994-302513

XRPX Acc No: N92-298566

Recovery of computer program infected by virus - using unique fingerprint
of program which is stored along with data relating to beginning
portion of program

Patent Assignee: BRM TECHNOLOGIES LTD (BRMT-N); SYMANTEC CORP (SYMA-N)

Inventor: MANN O

Number of Countries: 018 Number of Patents: 007

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 514815	A2	19921125	EP 92108365	A	19920518	199248 B
CA 2069239	A	19921125	CA 2069239	A	19920522	199307
EP 514815	A3	19931222	EP 92108365	A	19920518	199515
US 5408642	A	19950418	US 91705390	A	19910524	199521
IL 101983	A	19951231	IL 101983	A	19920524	199614
EP 514815	B1	19971126	EP 92108365	A	19920518	199801
DE 69223275	E	19980108	DE 623275	A	19920518	199807
			EP 92108365	A	19920518	

Priority Applications (No Type Date): US 91705390 A 19910524

Cited Patents: No-SR.Pub; 3.Jnl.Ref

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
-----------	------	-----	----	----------	--------------

EP 514815	A2	E	20	G06F-011/00	
-----------	----	---	----	-------------	--

Designated States (Regional): AT BE CH DE DK ES FR GB GR IT LI LU NL PT
SE

US 5408642	A		14	G06F-011/08	
------------	---	--	----	-------------	--

EP 514815	B1	E	23	G06F-011/00	
-----------	----	---	----	-------------	--

Designated States (Regional): AT BE CH DE DK ES FR GB GR IT LI LU NL PT
SE

DE 69223275	E			G06F-011/00	Based on patent EP 514815
-------------	---	--	--	-------------	---------------------------

CA 2069239	A			G06F-011/10	
------------	---	--	--	-------------	--

EP 514815	A3			G06F-011/00	
-----------	----	--	--	-------------	--

IL 101983	A			G06F-011/00	
-----------	---	--	--	-------------	--

Abstract (Basic): EP 514815 A

A computer program that has been infected by a computer virus can
be recovered by use of a fingerprint. Prior to the program being
infected the program is examined and a fingerprint of the program is
taken along with initial data from the beginning of the program.

The fingerprint and beginning data is stored in a separate area
from the program and a backup version of the original program is also
stored. When the program is called a check is made on the original and
stored program fingerprints and in case of deviation the stored program
is restored.

USE - Computer program security and detection of virus .

Dwg.8/10

15/3,K/10 (Item 10 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01032563

DETECTION AND ELIMINATION OF MACRO VIRUSES

ERKENNUNG UND ENTFERNUNG VON MAKROVIREN

DETECTION ET ELIMINATION DE MACRO-VIRUS

PATENT ASSIGNEE:

SYMANTEC CORPORATION, (1606222), 20330 Stevens Creek Boulevard,
Cupertino, CA 95014, (US), (Proprietor designated states: all)

INVENTOR:

CHI, Darren, 637 Meridian Avenue, Alhambra, CA 91803, (US)

LEGAL REPRESENTATIVE:

Beresford, Keith Denis Lewis et al (28273), BERESFORD & Co. 2-5 Warwick
Court, High Holborn, London WC1R 5DH, (GB)

PATENT (CC, No, Kind, Date): EP 1012720 A1 000628 (Basic)

EP 1012720 B1 020116

WO 9909477 990225

APPLICATION (CC, No, Date): EP 98934333 980708; WO 98US14169 980708

PRIORITY (CC, No, Date): US 911298 970814

DESIGNATED STATES: DE; FR; GB

INTERNATIONAL PATENT CLASS: G06F-011/00

NOTE:

No A-document published by EPO

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
----------------	----------	--------	------------

CLAIMS B	(English)	200203	585
----------	-----------	--------	-----

CLAIMS B	(German)	200203	553
----------	----------	--------	-----

CLAIMS B	(French)	200203	665
----------	----------	--------	-----

SPEC B	(English)	200203	4075
--------	-----------	--------	------

Total word count - document A	0
-------------------------------	---

Total word count - document B	5878
-------------------------------	------

Total word count - documents A + B	5878
------------------------------------	------

...CLAIMS a simulated manner; and

a detection module (17), coupled to said emulator, and operable to
detect the presence of macro **viruses** based upon a preselected
decision criterion on the behaviour of the macros, and information
provided...

...of claim 1 further comprising:

coupled to said detection module, a repair module (19) for **eliminating**
macro **viruses** **detected** by said **detection** module.

3. A method for **detecting** the presence of macro **viruses** within a
digital computer (1), said method comprising the steps of:
associating an **application program** (5) with said digital computer;

associating a global environment (13) with said application program;
causing said application program to generate at...

...behaviour of the macros.

4. The method of claim 3, further comprising the step of **deleting** a
macro **virus** when said macro virus is deemed to be present.

5. The method of claim 3...

15/3,K/11 (Item 11 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01032272

Automated sample creation of macro viruses

Automatische Mustererzeugung von Makroviren

Creation automatisée des échantillons de macro virus

PATENT ASSIGNEE:

International Business Machines Corporation, (200128), New Orchard Road,

Armonk, NY 10504, (US) (Proprietor designated states 11)

INVENTOR:

Boulay, Jean-Michel Yann, 7 rue Edouard Stephan, 13004 Marseille, (FR)
Petrillo, August T., 32 Brett Lane, Bedford, New York 10506, (US)
Swimmer, Morton Gregory, 350 North Greeley Avenue, Chappaqua, New York
10514, (US)

LEGAL REPRESENTATIVE:

Boyce, Conor (74272), IBM United Kingdom Limited, Intellectual Property
Law, Hursley Park, Winchester, Hampshire SO21 2JN, (GB)

PATENT (CC, No, Kind, Date): EP 918285 A2 990526 (Basic)
EP 918285 A3 990922
EP 918285 B1 030326

APPLICATION (CC, No, Date): EP 98309016 981104;

PRIORITY (CC, No, Date): US 66382 P 971121; US 41493 980312

DESIGNATED STATES: DE; FR; GB

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: G06F-011/00

ABSTRACT WORD COUNT: 238

NOTE:

Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English

TEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	199921	595
CLAIMS B	(English)	200313	696
CLAIMS B	(German)	200313	720
CLAIMS B	(French)	200313	772
SPEC A	(English)	199921	6595
SPEC B	(English)	200313	6661
Total word count - document A			7191
Total word count - document B			8849
Total word count - documents A + B			16040

...ABSTRACT a system and method for automatically generating at least one instance of a computer macro **virus** that is native to or **associated** with an **application**. The method includes steps of (a) providing a suspect **virus** sample; and (b) replicating the suspect virus sample onto a least one goat file, using...

...additional instance of an infected goat file. The step of providing includes a step of **determining** attributes of the suspect **virus** sample, and the steps of exercising employ simulated user input or interprocess communication commands that...

CLAIMS 1. A method for automatically generating at least one instance of a computer macro **virus** **associated** with an **application**, comprising steps of:

providing a suspect **virus** sample; and
replicating the suspect **virus** sample onto a least one goat file, using at least one of simulated user input...

...A method as in claim 2, wherein the step of providing includes a step of **determining** attributes of the suspect **virus** sample, and wherein the steps of exercising use simulated user input or interprocess communication commands...

15/3,K/12 (Item 12 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

(c) 2004 European Patent Office. All rts. reserv.

00662890

Method and apparatus for detection of computer viruses
Verfahren und Gerat zur Erkennung von Computerviren
Procede et appareil de detection de virus d'ordinateurs

PATENT ASSIGNEE:

Chambers, David Alan, (1817400), 3655 Eastwood Circle, Santa Clara,

California 95054, (US) (Proprietor designated states (11))
INVENTOR:
Chambers, David Alan, 3655 Eastwood Circle, Santa Clara, California 95054
, (US)
LEGAL REPRESENTATIVE:
O'Connell, David Christopher et al (62551), Haseltine Lake & Co.,
Imperial House, 15-19 Kingsway, London WC2B 6UD, (GB)
PATENT (CC, No, Kind, Date): EP 636977 A2 950201 (Basic)
EP 636977 A3 970806
EP 636977 B1 010523
APPLICATION (CC, No, Date): EP 94305551 940727;
PRIORITY (CC, No, Date): US 99368 930729
DESIGNATED STATES: BE; DE; FR; GB; IT
INTERNATIONAL PATENT CLASS: G06F-011/00
ABSTRACT WORD COUNT: 114
FIGURE:
Figure number on first page: 1B

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF2	464
CLAIMS B	(English)	200121	593
CLAIMS B	(German)	200121	525
CLAIMS B	(French)	200121	665
SPEC A	(English)	EPABF2	5575
SPEC B	(English)	200121	5666
Total word count - document A			6040
Total word count - document B			7449
Total word count - documents A + B			13489

...ABSTRACT A2

A behavior analyzing **antivirus** program **detects** **viral** infection of a target program by emulating the execution of the target program and analyzing the emulated execution to **detect** **viral** behavior. The **antivirus** monitor **program** contains both variables **corresponding** to the CPU's registers and emulation procedures corresponding to the CPU's instructions. The target program is loaded into memory and its execution is emulated by the **antivirus** monitor program. Intelligent procedures contained in the monitor program are given control between every instruction...

...CLAIMS detected.

- The computer system of claim 1, wherein said computer system is configured to **detect** a computer **virus** **associated** with said target **program**, wherein said predetermined behavior is chosen to be indicative of replication of said computer **virus**.
- The computer system of claim 1 wherein said instruction emulation means comprises:
a register...

15/3,K/13 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

01099267 **Image available**

METHOD AND APPARATUS FOR DETECTING MALICIOUS CODE IN AN INFORMATION HANDLING SYSTEM

PROCEDE ET APPAREIL POUR DETECTER UN CODE MALVEILLANT DANS UN SYSTEME DE MANIPULATION D'INFORMATIONS

Patent Applicant/Assignee:

WHOLESECURITY INC, 5001 Plaza on the Lake, Suite 301, Austin, TX 78746,
US, US (Residence), US (Nationality)

Inventor(s):

OBRECHT Mark Eric, 2301 South Mopac #734, Austin, TX 78746, US,
ALAGNA Michael Anthony, 4424 Gaines Ranch Loop #130, Austin, TX 78735, US

PAYNE Charles Andrew, 1 Rialto Boulevard #1736, Austin, TX 78735, US,
Legal Representative:

DAVIS JR Michael A (et al) (agent), Haynes and Boone, LLP, 901 Main
Street, Suite 3100, Dallas, TX 75202-3789, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200421197 A1 20040311 (WO 0421197)

Application: WO 2003US26993 20030826 (PCT/WO US03026993)

Priority Application: US 2002231557 20020830; US 2003647644 20030825

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU

CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP

KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PG PH PL

PT RO RU SC SD SE SG SK SL SY TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM

ZW

(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE

SI SK TR

(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 8691

Fulltext Availability:

Claims

Claim

... of the examined characteristics and behaviors, the assigned weights
indicative of a valid program or **malicious code** as a function of the
detection
routines; and
determining whether executable code under investigation is malicious code
as a function
of...

...detection routines.

22 The method of claim 21, wherein the detection routines include valid
program **detection** routines and **malicious code detection** routines.

23 The method of claim 21, wherein the valid program detection routines
determine whether the executable code under investigation exhibits at
least one or more characteristics and
behaviors **associated** with a valid program; and
wherein the **malicious code detection** routines **determine** whether
the executable code under investigation exhibits at least one or more
characteristics and behaviors...

...weights.

25 The method of claim 24, wherein scoring includes using a scoring
algorithm for **identifying** executable code as **malicious code** in
response to at least one of a valid score and a malicious code score...

... of the examined characteristics and behaviors, the assigned weights
indicative of a valid program or **malicious code** as a function of the
detection routines;
and
determine whether executable code under investigation is malicious code as
a function of...

...weights.

50 The computer program of claim 49, wherein the detection routines
include valid
program **detection** routines and **malicious code detection** routines.

51 The computer program of claim 49, wherein the valid program detection
routines determine whether the executable code under investigation

exhibits at least one more characteristics and behaviors associated with a valid program; and wherein the malicious code detection routines determine whether the executable code under investigation exhibits at least one or more characteristics and behaviors...

...53 The computer program of claim 52, wherein scoring includes using a scoring algorithm for identifying executable code as malicious code in response to at least one of a valid score and a malicious code score...

...of the examined characteristics and behaviors, the assigned weights indicative of a valid program or malicious code as a function of the detection routines; and determine whether executable code under investigation is malicious code as a function of...

...78 The information handling system of claim 77, wherein the detection routines include valid program detection routines and malicious code detection routines.

...The information handling system of claim 77, wherein the valid program detection routines...

...whether the executable code under investigation exhibits at least one or more characteristics and behaviors associated with a valid program; and wherein the malicious code detection routines determine whether the executable code under investigation exhibits at least one or more characteristics and behaviors...

...The information handling system of claim 80, wherein scoring includes using a scoring algorithm for identifying executable c(' - s malicious code in response to a valid score and a malicious code score.

82 The information handling...

15/3,K/14 (Item 2 from file: 349)
 DIALOG(R)File 349:PCT FULLTEXT
 (c) 2004 WIPO/Univentio. All rts. reserv.

01055594 **Image available**
 USING DISASSOCIATED IMAGES FOR COMPUTER AND STORAGE RESOURCE MANAGEMENT
 UTILISATION D'IMAGES DISSOCIEES POUR LA GESTION DE RESSOURCES MEMOIRE ET INFORMATIQUES

Applicant/Assignee:

POWERQUEST CORPORATION, Building K, 1359 N. Research Way, Orem, UT 84097,
 US, US (Residence), US (Nationality), (For all designated states
 except: US)

Patent Applicant/Inventor:

KLEINSCHNITZ Donald Jr, 3142 East Fawnwood Cove, Sandy, UT 84092, US, US
 (Residence), US (Nationality), (Designated only for: US)
 ARBON Val A, 1276 East 620North, Orem, UT 84097, US, US (Residence), US
 (Nationality), (Designated only for: US)
 WHATCOTT Roland D, 39 West 800 South, Salem, UT 84653, US, US (Residence)
 , US (Nationality), (Designated only for: US)

Legal Representative:

OGILVIE John W L (agent), Computer Law++, 1211 East Yale Avenue, Salt
 Lake City, UT 84105, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200385526 A1 20031016 (WO 0385526)
 Application: WO 2003US10197 20030402 (PCT/WO US0310197)
 Priority Application: US 2002370100 20020403

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU
 CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP
 KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO
 RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
 (EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE

SI SK TR

(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 14287

Fulltext Availability:

Claims

Claim

... disk usage information, determining whether a particular file is present, determining whether at least one file of a particular type is present, determining billing for storage usage, detecting a virus-infected file, identifying an illegal file, identifying a breach of a policy that defines standardized storage locations for...

15/3,K/15 (Item 3 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2004 WIPO/Univentio. All rts. reserv.

01032995 **Image available**

COMPUTER VIRUS EXTERMINATION METHOD AND COMPUTER VIRUS DETECTION DISPLAY METHOD

PROCEDE D'EXTERMINATION D'UN VIRUS INFORMATIQUE ET PROCEDE DE PRESENTATION DE VIRUS INFORMATIQUES DETECTES

Patent Applicant/Assignee:

JAPAN SCIENCE AND TECHNOLOGY CORPORATION, 1-8, Hon-cho 4-chome, Kawaguchi-shi, Saitama 332-0012, JP, JP (Residence), JP (Nationality), (For all designated states except: US)

Patent Applicant/Inventor:

KOUI Yuuji, 17-48-505, Aoyama 4-chome, Morioka-shi, Iwate 020-0133, JP, JP (Residence), JP (Nationality), (Designated only for: US)
NAKAYA Naoshi, 3-4 Iwate Daigaku Kitayama Shukusha, 14-36, Kitayama 2-chome, Morioka-shi, Iwate 020-0061, JP, JP (Residence), JP (Nationality), (Designated only for: US)

Legal Representative:

NISHIURA Tsuguharu (agent), NISHIURA & ASSOCIATES, Toranomom 19 MT Building 6F, 2-20, Toranomom 1-chome, Minato-ku, Tokyo 105-0001, JP,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200362990 A1 20030731 (WO 0362990)

Application: WO 2003JP669 20030124 (PCT/WO JP0300669)

Priority Application: JP 200217777 20020125; JP 200315789 20030124

Designated States: CA US

Publication Language: Japanese

Filing Language: Japanese

English Abstract

...manual operation by a user. In a computer communication device installed, there is prepared an anti-virus program having a function to detect existence of a particular computer virus, a function to exterminate the computer virus, and a function to have an infection ability identical or substantially identical to the particular...

...infection ability and transmit its clone to another computer communication device when the particular computer virus is exterminated. An anti-virus program is installed in at least one computer communication device connected to a communication network and infected with a particular computer virus. Through the infection route of the particular computer virus, the anti-virus program clone is distributed to infect the other computer communication devices one after another (ST3, ST4).

15/3,K/16 (Item 4 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

00952577 **Image available**

COMPUTER VIRUS CHECK DEVICE AND METHOD

DISPOSITIF ET PROCEDE DE DETECTION DE VIRUS INFORMATIQUES

Patent Applicant/Assignee:

XAXON R & D CORPORATION, Ohtemachi Tatemono Kamiyacho Building 5th Floor,
12-13, Toranomom 5-chome, Minato-ku, Tokyo 105-0001, JP, JP (Residence)
, JP (Nationality), (For all designated states except: US)

Patent Applicant/Inventor:

YOSHII Kiyotoshi, c/o XAXON R & D CORPORATION, Ohtemachi Tatemono
Kamiyacho Building 5th Floor, 12-13, Toranomom 5-chome, Minato-ku,
Tokyo 105-0001, JP, JP (Residence), JP (Nationality), (Designated only
for: US)

Legal Representative:

OHKI Kenichi (agent), OHKI PATENT OFFICE, 15-1-205, Yushima 2-chome,
Bunkyo-ku, Tokyo 113-0034, JP,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200286717 A1 20021031 (WO 0286717)

Application: WO 2002JP3645 20020412 (PCT/WO JP0203645)

Priority Application: JP 2001116347 20010416; JP 2001184010 20010618; JP
2001196108 20010620; JP 2001213484 20010713; JP 2001234498 20010802

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU

CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP

KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO

RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 9400

Fulltext Availability:

Claims

Claim

... and distributes said task information among each of said pattern
matching circuits.

4 A computer **virus check** device according to claim 1, wherein, when
there are two or more of said pattern...

...and distributes the divided file among each of said pattern matching
circuits.

5 A computer **virus check** device according to claim 1, wherein, when
there are two or more of said pattern pattern data **corresponding** to the
file among each of said pattern matching circuits.

6 A computer **virus check** device according to claim 1, further
comprising a network interface

1 9

circuit including a...

...a PHY (Physical Layer).

7 A semiconductor integrated circuit having any one of the computer
virus check devices according to claims 1 to 6 integrated into a
single chip.

8 A computer comprising two or more of a computer **virus check** device
comprising: a task queue memory for receiving and saving file information
uniquely specifying a...

00945796 **Image available**

**SYSTEM AND METHOD FOR RESTORING COMPUTER SYSTEMS DAMAGED BY A MALICIOUS
COMPUTER PROGRAM**

**SYSTEME ET TECHNIQUE DE REMISE EN ETAT DE SYSTEMES INFORMATIQUES ENDOMMAGES
PAR UN PROGRAMME D'ORDINATEUR MALVEILLANT**

Patent Applicant/Assignee:

COMPUTER ASSOCIATES THINK INC, One Computer Associates Plaza, Islandia,
NY 11749, US, US (Residence), US (Nationality)

Inventor(s):

MALIVANCHUK Taras, Zalman Aran 24/5 St., Holon, IL,
LAFEL Moshe, Gutman 14 St., Petach Tikva, IL,
KATSHFIELD Ofer, Yigal Alon 7 St., Kiryat Uno, IL,

Legal Representative:

JAWORSKI Richard F (agent), Cooper & Dunham LLP, 1185 Avenue of the
Americas, New York, NY 10036, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200279956 A1 20021010 (WO 0279956)

Application: WO 2002US9414 20020326 (PCT/WO US0209414)

Priority Application: US 2001823673 20010330

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU

CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP

KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO

RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 4964

Fulltext Availability:

Claims

English Abstract

A method for restoring a computer system modified by malicious code. The
method **scans** the computer system for the **malicious code** ,
identifies the **malicious code** and retrieves from a data **file** ,
information **relating** to the **malicious code** including at least one
command used for restoring the computer system to a state that...

Claim

... restoring a computer system modified by malicious code, comprising:
scanning the computer system for the **malicious code** ;
identifying the **malicious code** ;
retrieving from a data **file** , information **relating** to the **malicious
code** including at least one command used for restoring the computer
system to a state that...of claim 1, wherein the data file comprises a
plurality of data files, each data **file** being provided for a
particular type of **malicious code** , each ...computer executable code
for restoring a computer system
modified by malicious code, comprising:
code for **scanning** the computer system for the **malicious code** ;
code for **identifying** the **malicious code** ;
code for retrieving from a data **file** , information **relating** to the
malicious code including at least one command used for restoring the
computer system to a state that...of claim 6, wherein the data file
comprises a plurality of data files, each data **file** being provided for
a **particular** type of **malicious code** , each data file including at
least one command that can be used for restoring the...for restoring a
computer system modified by malicious code, comprising: a data signal
portion for **scanning** the computer system for the **malicious code** ;
a data signal portion for **identifying** the **malicious code** ;
a data signal portion for retrieving from a data **file** , information
relating to the **malicious code** including at least one command used

for restoring the computer system to a state that...claim 1, wherein the data file comprises a plurality of data files, each data file being provided for a particular type of malicious code, each data file including at least one command that can be used for restoring code, comprising:
means for scanning the computer system for the malicious code;
means for identifying the malicious code;
means for retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer system to a state that...

15/3,K/18 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00884966 **Image available**

MAINTAINING VIRUS DETECTION SOFTWARE

MISE A JOUR D'UN LOGICIEL DE DETECTION DE VIRUS

Patent Applicant/Assignee:

F-SECURE OYJ, Tammasaarankatu 7, PL 24, Helsinki, FIN-00180 Helsinki, FI,
FI (Residence), FI (Nationality), (For all designated states except:
US)

Patent Applicant/Inventor:

HYPPONEN Ari, Joutsenpolku 25, FIN-10160 Degerby, FI, FI (Residence), FI
(Nationality), (Designated only for: US)

Legal Representative:

LIND Robert (agent), Marks & Clerk, 4220 Nash Court, Oxford Business Park
South, Oxford, Oxfordshire OX4 2RU, GB,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200219067 A2-A3 20020307 (WO 0219067)

Application: WO 2001EP9643 20010820 (PCT/WO EP0109643)

Priority Application: GB 200021278 20000831

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU

CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP

KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD

SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 3652

Fulltext Availability:

Claims

English Abstract

A method of managing a virus signature database associated with an anti-virus application, both of which are resident in a memory of a mobile wireless device 2,4...

...4. In accordance with instructions contained in the management messages, individual signature entries of the virus signature database are deleted or replaced, and new signatures added.

Claim

1 A method of managing a virus signature database associated with an anti-virus application, both of which are resident in a memory of a computer device, the method comprising...

...and comprising

receiving management messages over the wireless interface, the management messages containing respective add, delete, or replace virus signature instructions.

4 A method according to claim 3, wherein in the case of an...

...communicate with a cellular telecommunications network.

9 A computer device having a memory and an **anti - virus** software application resident in the memory, the memory also containing an **anti - virus** signature database accessible in use by the **anti - virus** application, the apparatus comprising processing means for adding, deleting, and/or replacing individual signature entries...

...wherein the computer device is a mobile wireless device.

11 A method of managing a **virus** signature database **associated** with an **anti - virus** , **application** , both of which are resident in a memory of a mobile wireless device, the method comprising receiving management messages, **relating** to database or **anti - virus** **application** changes, at the device, the management messages being filtered either at the origin side of...

15/3,K/19 (Item 7 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00884965 **Image available**

VIRUS PROTECTION IN AN INTERNET ENVIRONMENT
PROTECTION ANTI-VIRUS DANS UN ENVIRONNEMENT INTERNET

Patent Applicant/Assignee:

F-SECURE OYJ, Tammasaarankatu 7, PL 24, Helsinki, FIN-00180 Helsinki, FI,
FI (Residence), FI (Nationality), (For all designated states except:
US)

Patent Applicant/Inventor:

SAMMAN Ben, 31, rue ST Andre des Arts, F-75006 Paris, FR, FR (Residence),
US (Nationality), (Designated only for: US)

Legal Representative:

LIND Robert (agent), Marks & Clerk, 4220 Nash Court, Oxford Business Park
South, Oxford, Oxfordshire OX4 2RU, GB,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200219066 A2-A3 20020307 (WO 0219066)

Application: WO 2001EP9642 20010820 (PCT/WO EP0109642)

Priority Application: GB 200021280 20000831

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU

CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP

KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PH PL PT RO RU

SA SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW

RU; AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 3313

Fulltext Availability:

Claims

Claim

... accessible to said browser:

creating an instance of a browser plugin, said plugin providing a **virus**
scanning

function or providing a route to a **virus scanning** function;

scanning the data for **viruses** using the instance of the plugin;

if no **viruses** are **detected** in the data, returning the data to the
browser for

1 0 rendering; and

if a **virus** is **detected** in the data, inhibiting rendering of the data.

2 A method according to claim 1...

...4 A method according to any one of the preceding claims, wherein the

plugin comprise virus scanning functionality.

5 A method according to any one of claims 1 to 3, wherein the instance of the plugin created by the browser causes a separate virus scanning application to be opened, and the plugin makes the data accessible to the scanning application...

...mobile wireless device comprising a memory having a WAP browser application stored therein and a virus scanning browser plugin, wherein in use the WAP browser creates an instance of the virus scanning plugin for scanning WAP data prior to rendering the data.

7 A mobile wireless device comprising a memory...

15/3,K/20 (Item 8 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00559337

METHOD AND APPARATUS FOR COMPUTER VIRUS DETECTION, ANALYSIS, AND REMOVAL IN REAL TIME

PROCEDE ET APPAREIL DE DETECTION, ANALYSE ET SUPPRESSION DE VIRUS INFORMATIQUE EN TEMPS REEL

Patent Applicant/Assignee:

CYBERSOFT INC,

Inventor(s):

WELLS Joseph M,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200022710 A2 20000420 (WO 0022710)

Application: WO 99US22445 19990928 (PCT/WO US9922445)

Priority Application: US 98163251 19980930

Designated States: CA AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE

Publication Language: English

Fulltext Word Count: 4413

Fulltext Availability:

Claims

Claim

... in claim 1, wherein said system is configured, in the 0 event of a known virus being detected, to use relational data process to invoke the known-virus verification and removal process for the specific virus detected.

8 The computer system in claim 1, wherein said system is configured in any one...

15/3,K/21 (Item 9 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00501621 **Image available**

METHOD FOR IDENTIFYING VALIDITY OF AN EXECUTABLE FILE DESCRIPTION

PROCEDE D'IDENTIFICATION DE LA VALIDITE DE LA DESCRIPTION D'UN FICHIER EXECUTABLE

Patent Applicant/Assignee:

SQUARE D COMPANY,

Inventor(s):

TATE Allan R,

SAYLOR Michael J,

GROSSER John T,

Patent and Priority Information (Country, Number, Date):

Patent: WO 9932973 A1 19990701

Application: WO 98US27220 19981222 (PCT/WO US9827220)

Priority Application: US 97995711 19971222

Designated States: CA MX AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT

SE

Publication Language: English
Fulltext Word Count: 4636

English Abstract

...the integrity of the file to be verified at any time and is used to **detect viruses** or corrupted or tampered files at startup and also during runtimes of the file and its **associated application**. The operating system will store the new file length in a file allocation table and...

15/3,K/22 (Item 10 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00478125 **Image available**

DETECTION AND ELIMINATION OF MACRO VIRUSES
DETECTION ET ELIMINATION DES MACRO-VIRUS

Applicant/Assignee:

HEWLETTCORPORATION,

Inventor(s):

CHI Darren,

Patent and Priority Information (Country, Number, Date):

Patent: WO 9909477 A1 19990225

Application: WO 98US14169 19980708 (PCT/WO US9814169)

Priority Application: US 97911298 19970814

Designated States: CA JP AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT

SE

Publication Language: English

Fulltext Word Count: 4831

Fulltext Availability:

Claims

English Abstract

Apparatus and method for **detecting** the presence of macro **viruses** within a digital computer (1). An **application program** (5) is **associated** with the digital computer (1). A global environment (13) is associated with the application program...

Claim

Claims

1 Apparatus for **detecting** macro viruses, said apparatus comprising:

a digital computer having at least one storage device;
an application program **associated** with said computer;
a global environment associated with said application
1 0 program;
at least...

...apparatus of claim 1 further comprising:

coupled to said emulator, a detection module adapted to **detect** the presence of macro **viruses** based upon a preselected 20 decision criterion and based upon information provided by said emulator...

...apparatus of claim 2 further comprising:

coupled to said detection module, a repair module for **eliminating** macro **viruses** **detected** by said **detection** module.

4 A method for **detecting** the presence of macro **viruses** within a digital computer, said method comprising the steps of:
associating an **application program** with said digital computer;

1 5

associating a global environment with said application program;

causing...

...deemed to be present.

5 The method of claim 4 further comprising the step of
deleting a macro virus when said macro virus is deemed to be
present.

19/5,K/26 (Item 16 from file: 349)
DIALOG(R) File 349:PCT FULLTEXT
(C) 2004 WIPO/Univentio. All rts. reserv.

00451455 **Image available**

VIRUS DETECTION IN CLIENT-SERVER SYSTEM

DETECTION DE VIRUS DANS UN SYSTEME CLIENT/SERVEUR

Patent Applicant/Assignee:

TREND MICRO INCORPORATED,

CHEN Eva,

Inventor(s):

CHEN Eva,

LAU Steven Yuen-Lam,

LIANG Yung-Chang,

Patent and Priority Information (Country, Number, Date):

Patent: WO 9841919 A1 19980924

Application: WO 98US3796 19980313 (PCT/WO US9803796)

Priority Application: US 97820649 19970318

Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES

FI GB GE GH GM GW HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD

MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ

VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH

DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR

NE SN TD TG

Main International Patent Class: G06F-011/00

International Patent Class: G06F-11:22

Publication Language: English

Fulltext Availability:

Detailed Description

Claims

Fulltext Word Count: 17595

English Abstract

The iterative detection and treatment of viruses using virus detection objects and virus treatment objects is disclosed. Pursuant to a request for a virus scan, a virus detection object is produced by a server (400) and is transmitted to a client (300A, B) for execution. The client (300A, B) receives and executes the virus detection object, and the results are transmitted to the server (400). The server (400) uses the results to produce an additional virus detection object which is also transmitted to the client (300A, B) and executed so that the results can be transmitted to the server (400). The iterative production and execution of virus detection objects is continued until a determination is made as to whether the targeted file or data includes a virus. Upon a determination that a targeted file or data includes a virus, a vaccine specifically tailored to the conditions presented at the client (300A, B) and the type of virus detected is produced, preferably in the form of a virus treatment object. The request for a virus scan can be directly made or indirectly by a triggering event. One virus detection server (400) embodiment includes a virus information expert system that applies conditional data to predetermined knowledge about virus scanning to make determinations such as when to scan for viruses. A network diagnosis and treatment application includes a diagnostic data module, an expert system, and a maintenance requesting module. The expert system applies the diagnostic data to predetermined knowledge about the diagnosis and maintenance of a network to make determinations upon which maintenance requests are made. Preferably, the expert system includes a virus information expert system.

French Abstract

Detection iterative et traitement de virus au moyen d'objets de detection de virus et d'objets de traitement de virus. Suite a une demande de recherche de virus, un objet de detection de virus est produit par un serveur (400) et transmis a un client (300A, B) pour execution. Le client (300A, B) recoit et execute l'objet de detection de virus et les resultats sont transmis au serveur (400). Le serveur (400) utilise ces resultats pour produire un objet de detection de virus complementaire qui est egalement transmis au client (300A, B) et execute de sorte que les

resultats sont transmis au serveur (400). La production et l'execution iterative d'objets de detection de virus est poursuivie jusqu'a determination de la presence, le cas echeant, d'un virus dans le fichier ou dans les donnees cibles. S'il est determinee que le fichier ou les donnees cibles contiennent un virus, un vaccin specialement adapte aux conditions relevees chez le client (300A, B) et au type de virus detecte est produit, de preference sous forme d'un objet de traitement de virus. La demande de recherche de virus peut etre formulee directement ou indirectement par un evenement declenchant. Dans un mode de realisation, le serveur (400) de detection de virus comprend un systeme expert d'information sur les virus qui applique les donnees conditionnelles a ses connaissances predeterminees relatives a la recherche de virus pour determiner notamment quand rechercher les virus. Une application pour le diagnostic et le traitement d'un reseau comporte un module de donnees de diagnostic, un systeme expert et un module de demande de mise a jour. Le systeme expert applique les donnees de diagnostic aux connaissances predeterminees relatives au diagnostic et a l'entretien d'un reseau pour etablir des conclusions sur la base desquelles des demandes d'entretien sont formulees. Le systeme expert comprend de preference un systeme expert d'information sur les virus.

Main International Patent Class: G06F-011/00

International Patent Class: G06F-11:22

Fulltext Availability:

Detailed Description

Detailed Description

... scan is initiated without a request that it apparent to the user.

Once it is **determined** by the virus detection server that a valid virus detection request has been received, the...

...conditions presented at the client, including the specific type of virus that was detected. The **virus detection** server receives the results produced by the execution of one or more **virus detection** objects and analyses the results to tailor the vaccine. For example, the result may indicate that...system administrator. Specifically, events that regularly can be used to trigger a request for **virus scanning** by the **virus detection** server.

An embodiment of the **virus detection** server includes various modules for the iterative **detection** and treatment of computer **viruses**. An iterative **virus detection** module includes a **scanning** module, a **virus pattern** module, a virus rules module, a cleaning module, a cleaning pattern module, an access...can be used for the browser 330 and to provide the executable portions of the **virus detection** objects. For example, the browser 330 could be the Netscape Navigator as provided by...

...objects produced by the virus detection server 400, such as via an enabled browser 330, **viruses** can be **detected** and treated at the client 300 using the **virus detection** server 400.

Since **viruses** can be **detected** and treated at the client 300 using the **virus detection** server 400 using the enabled browser 330 (or other means to execute the **virus detection** objects), **viruses** can be **detected** and treated without the **virus detection** shell 332.

However, although the **virus detection** shell 332 is optional, it can alternatively be provided in memory 314 for various purposes...configured to acquire the necessary information.

After it is determined that a valid request for **scanning** has been provided, virus detection objects are iteratively produced and transmitted to the requester, such as a client 300, in order to detect a **virus**. The **scanning** module 454 includes various routines that can be used in the **detection** of **viruses**. Preferably, the routines are

provided for separate access so that virus detection objects can be tailored to include selected scanning routines. For example, separate routines for the detection of viruses that could reside in systems using particular platforms and operating systems, in particular file types...

...locations are provided for separate access in the scanning module 454. Specifically, routines for the detection of viruses that typically reside on one platform are provided such that they can be accessed separate from routines for the detection of viruses that typically reside on another platform. Similarly, routines for the detection of viruses that reside in "executable" files (such as those that have the file extension .exe) are provided such that they can be accessed separate from routines used for the detection of macro viruses (such as those that implement the WordBasic programming language, typically reside in application data files...

...in the scanning module are configured to use the particular programming tools used by the virus detection server 400 to detect viruses at the client 300. Thus, the routines are capable...to Fig. 5. Conventional indexing and sorting techniques can be used to tag the various virus scanning routines provided in the scanning module 454 and, accordingly, to facilitate separate access.

Similar to the scanning module 454, the virus pattern module 456 and virus rules module 458 respectively include virus signatures and rules that can be used in the detection of viruses. As with the routines described in connection with the scanning module 454, the patterns and rules are provided to facilitate separate access. Thus, for example, the file signatures in the virus pattern module 456 corresponding to one type of file can be separated from the virus signatures corresponding to a second file type. Similarly, the rules in the virus rules module 458 corresponding to one detection criteria can be separated from the virus rules...

File 348:EUROPEAN PATENT 978-2004/May W01

(c) 2004 European Patent Office

File 349:PCT FULLTEXT 1979-2002/UB=20040506,UT=20040429

(c) 2004 WIPO/Univentio

Set	Items	Description
S1	101801	VIRUS?? OR VIRII OR VIRAL OR MACROVIRUS?? OR TROJAN()HORSE- ?? OR WORM?? OR (MALICIOUS OR HOSTILE OR SUSPECT)() (LOGIC OR - CODE OR SOFTWARE OR PROGRAM?? OR ALGORITHM? ? OR COMMAND? ? OR SIGNAL? ? OR INSTRUCTION? ?)
	17203	S1(5N) (SCAN???? OR DETECT??? OR FIND??? OR SENS??? OR IDEN- TIF???? OR IDENTIFICATION OR DISCOVER? OR RECOGNI????? OR DET- ERMIN? OR CHECK???)
S3	11456	S1(5N) (DELET??? OR ERAS??? OR EXTERMINAT? OR REMOV??? OR D- ESTROY? OR KILL??? OR PURG??? OR ERADICAT? OR DISINFECT? OR E- LIMINAT? OR CLEAR??? OR CLEAN??? OR FLUSH???)
S4	7402	ANTIVIRUS OR ANTI() (VIRUS OR VIRAL)
S5	14914	(TAILOR? OR CUSTOMIZ? OR CUSTOMIS? OR INDIVIDUALIZ? OR IND- IVIDUALIS? OR PERSONALIZ? OR PERSONALIS? OR GEAR???) (5N) (PROC- ESS OR PROCESSES OR THREAD? ? OR PROGRAM? ? OR APPLICATION? ? OR FILE? ? OR FILETYPE? ?)
S6	409686	(SPECIFIC OR PARTICULAR OR CORRESPOND? OR CORRELAT? OR ASS- OCIAT? OR REFER??? OR RELATE? ? OR RELATING) (5N) (PROCESS OR P- ROCESSES OR THREAD? ? OR PROGRAM? ? OR APPLICATION? ? OR FILE? ? OR FILETYPE? ?)
S7	40	S2:S4(100N)S5
S8	1485	S2:S4(100N)S6
S9	239	S8 AND IC=G06F
S10	231	S9 NOT S7
S11	2468	S1(15N)S6
S12	634	S2:S4(100N)S11
S13	124	S12 AND IC=G06F
S14	118	S13 NOT S7
S15	22	S14/TI, AB, CM
S16	96	S14 NOT S15
S17	12	S16 AND IC=G06F-017
S18	84	S16 NOT S17
S19	32	S18 AND IC=G06F-011
S20	52	S18 NOT S19

File 275:Gale Group Computer DB(TM) 1983-2004/May 14
(c) 2004 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2004/May 13
(c) 2004 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2004/May 14
(c) 2004 The Gale Group
File 16:Gale Group PROMT(R) 1990-2004/May 14
(c) 2004 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
(c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2004/May 14
(c)2004 The Gale Group
File 624:McGraw-Hill Publications 1985-2004/May 13
(c) 2004 McGraw-Hill Co. Inc
File 15:ABI/Inform(R) 1971-2004/May 14
(c) 2004 ProQuest Info&Learning
File 647:CMP Computer Fulltext 1988-2004/May W1
(c) 2004 CMP Media, LLC
File 674:Computer News Fulltext 1989-2004/May W1
(c) 2004 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2004/May 13
(c) 2004 The Dialog Corp.
File 369:New Scientist 1994-2004/May W2
(c) 2004 Reed Business Information Ltd.
File 810:Business Wire 1986-1999/Feb 28
(c) 1999 Business Wire
File 813:PR Newswire 1987-1999/Apr 30
(c) 1999 PR Newswire Association Inc
File 610:Business Wire 1999-2004/May 14
(c) 2004 Business Wire.
File 613:PR Newswire 1999-2004/May 14
(c) 2004 PR Newswire Association Inc

Set	Items	Description
S1	355481	VIRUS?? OR VIRII OR VIRAL OR MACROVIRUS?? OR TROJAN()HORSE- ?? OR WORM?? OR (MALICIOUS OR HOSTILE OR SUSPECT)() (LOGIC OR - CODE OR SOFTWARE OR PROGRAM?? OR ALGORITHM? ? OR COMMAND? ? OR SIGNAL? ? OR INSTRUCTION? ?)
S2	63482	S1(5N) (SCAN???? OR DETECT??? OR FIND??? OR SENS??? OR IDEN- TIF???? OR IDENTIFICATION OR DISCOVER? OR RECOGNI????? OR DET- ERMIN? OR CHECK???)
S3	30122	S1(5N) (DELET??? OR ERAS??? OR EXTERMINAT? OR REMOV??? OR D- ESTROY? OR KILL??? OR PURG??? OR ERADICAT? OR DISINFECT? OR E- LIMINAT? OR CLEAR??? OR CLEAN??? OR FLUSH???)
S4	71193	ANTIVIRUS OR ANTI() (VIRUS OR VIRAL)
S5	254715	(TAILOR? OR CUSTOMIZ? OR CUSTOMIS? OR INDIVIDUALIZ? OR IND- IVIDUALIS? OR PERSONALIZ? OR PERSONALIS? OR GEAR???) (5N) (PROC- ESS OR PROCESSES OR THREAD? ? OR PROGRAM? ? OR APPLICATION? ? OR FILE? ? OR FILETYPE? ?)
S6	947379	(SPECIFIC OR PARTICULAR OR CORRESPOND? OR CORRELAT? OR ASS- OCIAT? OR REFER??? OR RELATE? ? OR RELATING) (5N) (PROCESS OR P- ROCESSES OR THREAD? ? OR PROGRAM? ? OR APPLICATION? ? OR FILE? ? OR FILETYPE? ?)
S7	645	S2:S4(100N)S5
S8	519	S1(15N)S5
S9	199	S2:S4(100N)S8
S10	177	S2:S4(50N)S8
S11	89	RD (unique items)
S12	66	S11 NOT PD>20000531
S13	3501	S2:S4(100N)S6
S14	256253	(SPECIFIC OR PARTICULAR) (7W) (PROCESS OR PROCESSES OR THREA- D? ? OR PROGRAM? ? OR APPLICATION? ? OR FILE? ? OR FILETYPE? - ?)
S15	1266	S2:S4(100N)S14
S16	899	S1(10N)S14
S17	402	S2:S4(100N)S16
S18	4364	(CORRESPOND? OR CORRELAT? OR ASSOCIAT? OR REFER??? OR RELA- TE? ? OR RELATING) (7W)S14

S19
S20

18 S2:S4(100N)S18
10 RD (unique items)

20/3,K/1 (Item 1 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2004 The Gale Group. All rts. reserv.

03647944 Supplier Number: 113806646 (USE FORMAT 7 FOR FULLTEXT)
U.S. Environmental Protection Agency Awards NanoBio(R) Contract For
Development of Anthrax Decontamination Product.
PR Newswire, pNA
March 2, 2004
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 451

NanoProtect's development plan will result in a safe bio-decontaminant that kills bacteria, viruses, spores and fungi while being uniquely non-toxic to humans or the environment. The EPA's specific interest relates to their Safe Buildings Program where NanoProtect would be used by first responders in the event of a bio-attack...

20/3,K/2 (Item 2 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2004 The Gale Group. All rts. reserv.

01183376 Supplier Number: 42689669 (USE FORMAT 7 FOR FULLTEXT)
VERTEX PHARMACEUTICALS RECEIVES NATIONAL SCIENCE FOUNDATION GRANT TO
DEVELOP NOVEL ENZYME TECHNOLOGY
PR Newswire, pl
Jan 23, 1992
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 397

... through which
synthetic compounds are designed at the atomic level to interact with
protein targets associated with particular disease processes

. Vertex
applies this approach, involving the integration of advanced biology,
chemistry, and biophysics to create...

...drugs to treat major diseases. The company is focusing on three major
therapeutic areas: immunology, anti viral chemotherapy, and
inflammation.

CONTACT: Richard H. Aldrich, 617-576-3111, vice president of Vertex;
or...

20/3,K/3 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

05032701 Supplier Number: 78375441 (USE FORMAT 7 FOR FULLTEXT)
Right Vision introduces new version of Eye-box ONE. (Brief Article) (Product
Announcement)
Internet Business News, pNA
Sept 18, 2001
Language: English Record Type: Fulltext
Article Type: Brief Article Product Announcement
Document Type: Magazine/Journal; Trade
Word Count: 176

... of a single box containing different modules that can be activated
when needed. The modules correspond to specific Internet applications
- such as web site hosting, e-mail, firewall and virtual private
networks. Additional modules, for anti-virus protection for instance,
can now also be purchased.

The new version comes with a step...

20/3,K/4 (Item 2 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

05081739 Supplier Number: 78375424 (USE FORMAT 7 FOR FULLTEXT)
Right Vision introduces new version of Eye-box ONE. (Eye-box ONE 2.5 network management software) (Brief Article) (Product Announcement)
Telecomworldwire, pNA
Sept 18, 2001
Language: English Record Type: Fulltext
Article Type: Brief Article Product Announcement
Document Type: Newsletter; Trade
Word Count: 189

... of a single box containing different modules that can be activated when needed. The modules correspond to specific Internet applications - such as web site hosting, e-mail, firewall and virtual private networks. Additional modules, for anti - virus protection for instance, can now also be purchased.

The new version comes with a step...

20/3,K/5 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

06059246 Supplier Number: 55349539 (USE FORMAT 7 FOR FULLTEXT)
In Search of Integrated Management. (Unicenter TNG, from Computer Associates leads in enterprise management solution race) (Product Information)
Steinke, Steve
Network, pNA
Dec 1, 1998
Language: English Record Type: Fulltext Abstract
Document Type: Magazine/Journal; Trade
Word Count: 3355

... the definition of business-process views, a select grouping of devices and processes that is associated with a particular business process. Depending on the degree of instrumentation installed on the individual objects, business-process views may...

...help desk product; ControlIT, a remote control product (formerly known as Remotely Possible); InoculateIT, an anti - virus tool (formerly Inoculan); and NetworkIT, an IP/IPX network manager.

The IT series of products...

20/3,K/6 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

04438109 Supplier Number: 46512710 (USE FORMAT 7 FOR FULLTEXT)
MicroHelp rushes toward compression utility market with Zip
InfoWorld, p090
July 1, 1996
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 737

... of WinZip that I especially like is it lets you run external programs, such as virus detectors and other archives. This feature doesn't exist in MicroHelp Zip -- or in Zip-It...

...text file that doesn't have an extension or a file whose extension is not associated with a specific program.

MicroHelp Zip does include password protection, but the manual makes

the encryption scheme sound as...

20/3,K/7 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

09048511 SUPPLIER NUMBER: 18741073 (USE FORMAT 7 OR 9 FOR FULL TEXT)
MicroHelp gets a base hit for its compression software. (Zip) (Software Review) (Evaluation) (Brief Article)
Byrne, Jason
Government Computer News, v15, n24, p38(1)
Sep 23, 1996
DOCUMENT TYPE: Evaluation Brief Article ISSN: 0738-4300
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 406 LINE COUNT: 00035

... the file back together.
Another complication is the inability to run external programs such as **virus scanners** in tandem. This hampers Zip's effectiveness for handling Internet files.
Must match
Viewers are...

...TXT but it's hardly useful otherwise. The same holds true for any file not **associated** with a **particular program**.
I found the interface easy to move through, and compression novices would find it hard...

20/3,K/8 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

08818516 SUPPLIER NUMBER: 18447202 (USE FORMAT 7 OR 9 FOR FULL TEXT)
MicroHelp rushes toward compression utility market with Zip. (MicroHelp Zip compression software for Windows) (Software Review) (Evaluation)
Peschel, Joe
InfoWorld, v18, n27, p90(1)
July 1, 1996
DOCUMENT TYPE: Evaluation ISSN: 0199-6649 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 769 LINE COUNT: 00063

... of WinZip that I especially like is it lets you run external programs, such as **virus detectors** and other archives. This feature doesn't exist in MicroHelp Zip -- or in Zip-It...

...text file that doesn't have an extension or a file whose extension is not **associated** with a **specific program**.
MicroHelp Zip does include password protection, but the manual makes the encryption scheme sound as...

20/3,K/9 (Item 3 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

05577467 SUPPLIER NUMBER: 11794018 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Free and User Supported Software for the IBM PC: A Resource Guide for Libraries and Individuals. (book reviews)
Grosch, Audrey N.
Library Software Review, v10, n6, p401(1)
Nov-Dec, 1991
DOCUMENT TYPE: review ISSN: 0742-5759 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT
WORD COUNT: 455 LINE COUNT: 00035

... will find excellent collections of free and user-supported software from reputable system operators who **virus** /operationally **check** their offerings or obtain them from the major electronic network distribution sources. In addition to the above SDN, there is the Software Distribution Service (SDS), WinNET for Windows- **specific programs** , and DvNET for DesQview- **related programs** . Ask your sysop about these as secure sources of this software. The authors would be...

20/3,K/10 (Item 4 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

03940947 SUPPLIER NUMBER: 07673495 (USE FORMAT 7 OR 9 FOR FULL TEXT)
The use of purified clotting factor concentrates in hemophilia.
Pierce, Glenn F.; Lusher, Jeanne M.; Brownstein, Alan P.; Goldsmith, Jonathan C.; Kessler, Craig M.
JAMA, The Journal of the American Medical Association, v261, n23, p3434(5)
June 16, 1989
ISSN: 0098-7484 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 4577 LINE COUNT: 00394

... with untreated or some dry-heated clotting factor concentrates (Table 1). Viral transmission is also **related** to other, less-well-studied factors **specific** to manufacturing **processes** as well as to the concentration of virus in the donor plasma pool and the...

...Table 2). In particular, the physical state of the clotting factor (dry, liquid) during the **viral** inactivation process affects **kill** of **virus** (Table 2). Products with lower specific activities, products heated to lower temperatures for less time...

...viruses. Therefore, the appropriate balance must be addressed between acceptable destruction of product and complete **elimination** of live **virus** . Informative data on the effects of stabilizers on viral kill and protein yield are considered...

File 3: Ei Compendex(R) 70-2004/May W1
 (c) 2004 Elsevier Eng. Info. Inc.
 File 35: Dissertation Abs Online 1861-2004/Apr
 (c) 2004 ProQuest Info&Learning
 File 202: Info. Sci. & Tech. Abs. 1966-2004/Feb 27
 (c) 2004 EBSCO Publishing
 File 65: Inside Conferences 1993-2004/May W2
 (c) 2004 BLDSC all rts. reserv.
 File 2: INSPEC 1969-2004/May W1
 (c) 2004 Institution of Electrical Engineers
 File 233: Internet & Personal Comp. Abs. 1981-2003/Sep
 (c) 2003 EBSCO Pub.
 File 94: JICST-EPlus 1985-2004/Apr W3
 (c) 2004 Japan Science and Tech Corp(JST)
 File 483: Newspaper Abs Daily 1986-2004/May 13
 (c) 2004 ProQuest Info&Learning
 File 6: NTIS 1964-2004/May W3
 (c) 2004 NTIS, Intl Cpyrght All Rights Res
 File 144: Pascal 1973-2004/May W1
 (c) 2004 INIST/CNRS
 File 434: SciSearch(R) Cited Ref Sci 1974-1989/Dec
 (c) 1998 Inst for Sci Info
 File 34: SciSearch(R) Cited Ref Sci 1990-2004/May W2
 (c) 2004 Inst for Sci Info
 File 99: Wilson Appl. Sci & Tech Abs 1983-2004/Apr
 (c) 2004 The HW Wilson Co.
 File 266: FEDRIP 2004/Mar
 Comp & dist by NTIS, Intl Copyright All Rights Res
 File 95: TEME-Technology & Management 1989-2004/Apr W4
 (c) 2004 FIZ TECHNIK
 File 438: Library Lit. & Info. Science 1984-2004/Apr
 (c) 2004 The HW Wilson Co

Set	Items	Description
S1	1033094	VIRUS?? OR VIRII OR VIRAL OR MACROVIRUS?? OR TROJAN()HORSE- ?? OR WORM?? OR (MALICIOUS OR HOSTILE OR SUSPECT)() (LOGIC OR - CODE OR SOFTWARE OR PROGRAM?? OR ALGORITHM? ? OR COMMAND? ? OR SIGNAL? ? OR INSTRUCTION? ?)
S2	89712	S1(5N) (SCAN???? OR DETECT??? OR FIND??? OR SENS??? OR IDEN- TIF???? OR IDENTIFICATION OR DISCOVER? OR RECOGNI????? OR DET- ERMIN? OR CHECK???)
S3	18310	S1(5N) (DELET??? OR ERAS??? OR EXTERMINAT? OR REMOV??? OR D- ESTROY? OR KILL??? OR PURG??? OR ERADICAT? OR DISINFECT? OR E- LIMINAT? OR CLEAR??? OR CLEAN??? OR FLUSH???)
S4	7952	ANTIVIRUS OR ANTI() (VIRUS OR VIRAL)
S5	26923	(TAILOR? OR CUSTOMIZ? OR CUSTOMIS? OR INDIVIDUALIZ? OR IND- IVIDUALIS? OR PERSONALIZ? OR PERSONALIS? OR GEAR???) (5N) (PROC- ESS OR PROCESSES OR THREAD? ? OR PROGRAM? ? OR APPLICATION? ? OR FILE? ? OR FILETYPE? ?)
S6	438344	(SPECIFIC OR PARTICULAR OR CORRESPOND? OR CORRELAT? OR ASS- OCIAT? OR REFER??? OR RELATE? ? OR RELATING) (5N) (PROCESS OR P- ROCESSES OR THREAD? ? OR PROGRAM? ? OR APPLICATION? ? OR FILE? ? OR FILETYPE? ?)
S7	45	S2:S4 AND S5
S8	34	RD (unique items)
S9	29	S8 NOT PY=2001:2004
S10	101148	(SPECIFIC OR PARTICULAR) (5W) (PROCESS OR PROCESSES OR THREA- D? ? OR PROGRAM? ? OR APPLICATION? ? OR FILE? ? OR FILETYPE? - ?)
S11	2135	(CORRESPOND? OR CORRELAT? OR ASSOCIAT? OR REFER??? OR RELA- TE? ? OR RELATING) (7W) S10
S12	27	S1 AND S11
S13	21	RD (unique items)
S14	19	S13 NOT (S9 OR PY=2001:2004)

14/5/3 (Item 1 from file: 202)
DIALOG(R)File 202:Info. Sci. & Tech. Abs.
(c) 2004 EBSCO Publishing. All rts. reserv.

2604297

Implementing optical storage.

Author(s): O'Connor, M A

Optical Information Systems vol. 11, no. 1, pages 39-41

Publication Date: Jan 1991

ISSN: 0886-5809

Language: English

Document Type: Journal Article

Record Type: Abstract

Journal Announcement: 2600

This article describes the uses of optical storage devices, and discusses how to implement specific applications. The author explores the various types of optical storage and the range of applications appropriate to each.

WORM, erasable, interactive videodisc, and optical memory card are studied. Issues associated with implementing optical technology are reviewed including issues associated with capture or conversion of data, and issues **associated** with **specific** database **applications**.

Descriptors: Disk storage; Optical disks

Classification Codes and Description: 5.07 (Storage)

Main Heading: Information Processing and Control

14/5/4 (Item 1 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.
(c) 2003 EBSCO Pub. All rts. reserv.

00291764 92PX10-024

Norton Desktop for Windows

Law, Greg

PCM, October 1, 1992, v10 n4 p10-12, 16, 3 Page(s)

ISSN: 0747-0460

Product Name: Norton Desktop for Windows

Languages: English

Document Type: Software Review

Grade (of Product Reviewed): B

Hardware/Software Compatibility: Microsoft Windows

Geographic Location: United States

WORKING IN WINDOWS column presents a favorable review of Norton Desktop for Windows v. 2.0 (\$NA), a user interface from Norton Utiliare of Pittsburgh, PA (412). Requires 8.5MB disk space. Says this program is a replacement for both the Windows Program Manager and File Manager. Installation is straightforward and easy. Supports most functions of File Manager and Program Manager and includes Norton Anti- **Virus**, Desktop Editor, Sleeper, Norton Disk Doctor, Scheduler, Norton Viewer, SuperFind, Smart Erase, Icon Editor, SysInfo, Batch Runner, Batch Builder, Macro Builder, Financial, Scientific, and Tape Calculators, Diskcopy, Key Finder, Format Disk, Shredder, and Norton Backup. Is better at copying and moving files and supports drag-and-drop techniques better than both Program Manager and File Manager. Can print files not **associated** with **specific** **applications**. Its best feature is that it is extendible. Contains six screen displays. (v1)